De La Salle University

Third-Party Security Risk Assessment and Rating

A Capstone Project Presented to
the Faculty of the College of Computer Studies
De La Salle University

In Partial Fulfillment
of the Requirements for the Degree of
Master in Information Security

by
Trinidad, Jovic O.

Mr. Gregory Cu
Faculty Adviser

April 7, 2023

De La Salle University

APPROVAL SHEET

This Thesis hereto entitled:

Third-Party Security Risk Assessment and Rating

_____

prepared and submitted by _____ JOVIC O. TRINIDAD _____

in partial fulfillment of the requirements for the degree of

Master in Information Security

_____

has been examined and is recommended for acceptance and approval for ORAL EXAMINATION.

MR. GREGORY CU
_____
Adviser

Approved by the Committee on Oral Examination with a grade of PASSED on

___ April 1, 2023 ___

MS. KATRINA YSABEL SOLOMON
_____
Chair

MR. JOHN FAUSTORILLA
_____
Member

MR. GREGORY CU
_____
Member

_____
Member

_____
Member

Accepted in partial fulfillment of the requirements for the degree of

Master in Information Security

_____

Dr. Rafael A. Cabredo
_____
Dean
College of Computer Studies

De La Salle University

Libraries

dipo

ANIMO REPOSITORY SUBMISSION CONSENT FORM A
UG/GS ETD Not Covered by DLSU Intellectual Property Policy Section 6.2 (2021)

The consent form below provides authorization for the permanent addition of ETDs to the Animo Repository for discoverability and wider dissemination of knowledge. A scanned copy of this form should be included as part of the preliminary pages of the ETD final PDF version.

I/we am/are executing this form in accordance with *Section 6.2 of the DLSU Intellectual Property Policy (2021).*

I/We hereby grant De La Salle University Libraries ("the Libraries") the royalty-free, non-exclusive license to manage and archive the work(s) identified below ("the submission") through the *Animo Repository* platform, subject to the provision of applicable laws.

Title of work   :   Third-party risk assesment and rating

I/We also grant the Libraries the right to make the full version of this submission accessible in electronic format for educational and research purposes only, based on the release permission below.

Release Permission (Please check only ONE box. *Please consult your thesis adviser before ticking any box.*)

☐ *Available to library patrons immediately (no embargo)*

☑ *Available to library patrons after the embargoed period (Choose this option if you and your thesis adviser intend to publish this work and/or protect your intellectual property. The metadata of your work will still be searchable in the Animo Repository during the embargo period.)*
  ☑ 1 year   ☐ 2 years   ☐ 3 years

☐ *Not available to library patrons (For storage only. However, the metadata of your work will still be searchable in the Animo Repository.)*

I/We agree that the Libraries may, without changing the content, convert and migrate this submission to any medium or format, and keep more than one copy for purposes of security, back-up, and preservation.

I/we am/are giving my/our consent for the Libraries to collect, store, and share my/our personal information, including my/our personal name, course, department, college, and institution, through the Animo Repository. I/we further agree that the personal data collected will only be used for the academic community and the general public to search, retrieve, and locate my/our work in the Animo Repository for educational and research purposes.

I/we understand that the security of the collected personal information shall be the responsibility of the Libraries and should comply with the requirements of RA 10173. I/we further consent that the personal data collected and included in the metadata in the Animo Repository will be permanently stored.

I/We further agree that this consent will remain in place unless I/we terminate it via signed communication with the Libraries.

I/We confirm that:
- The version I/we submitted is the final version approved by my/our thesis committee / panel.
- The submission is my/our original work and I/we have the right to grant the license above mentioned to the Libraries.

De La Salle University

Libraries

JOVIC O. TRINIDAD	APRIL 17, 2023
Student's Signature over Printed Name	Date
Student's Signature over Printed Name	Date
Student's Signature over Printed Name	Date
Student's Signature over Printed Name	Date
Student's Signature over Printed Name	Date
Student's Signature over Printed Name	Date
Student's Signature over Printed Name	Date
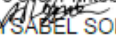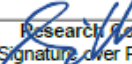
De La Salle University

Check the appropriate column for your answer.
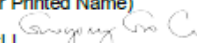
	I agree to have my name included and searchable in the Animo Repository.	I want to stay anonymous.
"As the thesis adviser, I have discussed with my advisee/s the contents of and reason for this form."		
GREGORY CU — 04/21/2023 **Thesis Adviser** (Signature over Printed Name) — Date	☑	☐
KATRINA YSABEL SOLOMON — 4/18/23 **Thesis Panel Member** (Signature over Printed Name) — Date	☑	☐
JOHN FRANCIS FAUSTORILLA — 4/19/2023 **Thesis Panel Member** (Signature over Printed Name) — Date	☑	☐
GREGORY CU — 04/21/2023 **Thesis Panel Member** (Signature over Printed Name) — Date	☑	☐
Research Coordinator (Signature over Printed Name) — Date	☐	☐
MARNEL PERADILLA — 04.21.2023 **Department Chair** (Signature over Printed Name) — Date	☑	☐

De La Salle University

Abstract

Organizations utilizing the applications and programs that were developed by a third-party supplier is on the rise. The combination of low-cost solution with the speed of implementation entices organizations to ditch the old model of hiring an entire team of individuals to internally develop applications that will fill-in their business needs. In trying to keep up with the digitization of competitors, organizations often overlook the cybersecurity risks a third-party supplier can potentially introduce to the existing information systems.

There is a gap on a standard process that will serve as a security checkpoint for all third-party developed programs and applications before they get onboarded to the organizations internal systems. For the target organization in this project, third-party applications sometimes do not go through the proper information security checks and implemented into the production environment without clearance from the information security team.

This initiative aims to fill this gap with a standard process to properly assess the vendor's information security capabilities, guide them with the proper security configuration of the application in compliance to the organization's minimum-security standards and to rate the vendor with a granular security matrix so that future engagements with a vendor can be properly assessed in the context of cybersecurity.